Exhibit D

Frequently Asked Questions

What is Tari Labs?   ▼

What is Tari?   ▼

Who are the investors behind Tari Labs?   ▼

What's the origin of the name "Tari"?   ▲

Tari literally means "newly minted money" in Arabic. It also refers to a small gold coin used in the Mediterranean from the 10th through the 14th centuries. Since it was lightweight and convenient to use compared with other coins of the time, it became a popular medium of exchange for everyday commerce. Similarly, we envision the new Tari protocol being commonly used to create and distribute digital assets of all types.

How is Tari Labs related to the Tari project?   ▼

Who are the co-founders of Tari Labs?   ▼

What's the story behind the Tari logo?   ▼

Where can I learn more / join the conversation?   ▼

Built in **Oakland** & **Johannesburg**

Submit

By clicking 'Submit', you agree to our Privacy Policy (/privacy_policy).

Home (/)   About (/about)

Join Us (/contribute)   Blog (/blog)

Newsletter (https://tari.substack.com/people/6766943)   FAQ (/faq)

Taro

⋮

Taro is a new Taproot-powered protocol for issuing assets on the bitcoin blockchain.

Taro is a new Taproot-powered protocol for issuing assets on the bitcoin blockchain that can be transferred over the Lightning Network for instant, high volume, low fee transactions. At its core, Taro taps into the security and stability of the bitcoin network and the speed, scalability, and low fees of Lightning.

Taro relies on Taproot, bitcoin's most recent upgrade, for a new tree structure that allows developers to embed arbitrary asset metadata within an existing output. It uses Schnorr signatures for improved simplicity and scalability, and, importantly, works with multi-hop transactions over Lightning.

Throughout Bitcoin's history, there have been a number of proposals with regard to bringing assets to the Bitcoin blockchain. Taro advances those ideas by focusing on what Taproot enables in that

≡ ⚡ **Builder's Guide**   🔍

channels, where nodes can offer atomic conversions from Bitcoin to Taro assets. This allows Taro assets to be interoperable with the broader Lightning Network, benefiting from its reach and strengthening its network effects.

Taro uses a Sparse-Merkle Tree to enable fast, efficient, private retrieval and updates to the witness/transaction data and a Merkle-Sum Tree to prove valid conservation/non-inflation. Assets can be transferred through on-chain transactions, or over the Lightning Network when deposited into a channel.

Participants in Taro transfer bear the costs of verification and storage by storing Taro witness data off-chain in local data stores or with information repositories termed "Universes" (akin to a git repository). To check a Taro asset's validity, its lineage since its genesis output is verified. This is achieved by receiving a verification file of transaction data through the Taro gossip layer. Clients can cross-check with their copy of the blockchain and amend with their own proofs as they pass on the asset.

3

What is Taro?

— A type of root vegetable
w/ a *taproot* structure

— Eaten across Africa,
South America, and Asia

— Great source of manganese,
potassium, and fiber

— Nigeria is the largest producer
of taro in the world

< 3 > ⋮   Google Slides

Summary:

1. Allows assets to be issued on the bitcoin blockchain

2. Leverages taproot for privacy and scalability

3. Assets can be deposited into Lightning channels

4. Assets can be transfered over the existing Lightning Network

Taro: A New Protocol for Multi-Asset Bitcoin and Lightning

4

📄 **Taro Protocol**

📄 **Taro on Lightning**

Features & Limitations

Taro allows for a long list of features that make the protocol scalable, robust, and friendly for low-powered mobile devices in situations of limited bandwidth.

- Taro is light client-friendly: has low verification costs and needs only access to untrusted bitcoin transactions. Taro does not require knowledge of the entire blockchain.

- Taro allows for atomic swaps between Taro assets and BTC

- Taro can handle both unique and non-unique assets as well as collections.

- Taro allows for creative multi-signature and co-signatory arrangements.

- Taro channels can be created alongside BTC channels in the same utxo, allowing Taro to exist in the Lightning Network without consuming additional resources. For instance, Alice can create two channels with Bob in a single Bitcoin transaction, one containing a Taro asset, the other BTC

- Future features may include confidential transactions and zero-knowledge proofs as part of Taro transfers.

📄 **Taro Protocol**

📄 **Taro on Lightning**

5

To learn more about the implementation of the Taro protocol, follow this link to the `tarod` client.

Further reading:

- Taro Q&A with Ryan Gentry - LNMarkets

←
Previous
Implementations and Links

Next
Taro Protocol
→

Last modified 4mo ago

WAS THIS PAGE HELPFUL? 😖 😐 😊